International Journal of Engineering & Scientific Research
Vol.5 Issue 3, March 2017,
ISSN: 2347-6532 Impact Factor: 5.900
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

REVIEW ON SECURITY AND CRYPTOGRAPHY

ER.ANUPAM BONKRA VIRK*

ABSTRACT

Security is of utmost importance in computers .The purpose of security is securing our data from unauthorized people. The security not only plays an important role in information technology, but it is also considered importantfor home, organization, bank, industries etc.

As compared to the traditional era, nowday's security measures are considered more due to the cropping up of criminal tendencies among techno savvy people.

Because of this hackers develop new hacking technologies for accessing the confidential data in any field, for destroying and removing those tendencies, Cryptography issued by authorized people against criminals.

The Cryptography is a technique which is used for the security of data in information technology. Basically it is act as protocol between users which are working on confidential data. The Cryptography is revolving around the various aspects of Information security such as data integrity, data confidentiality, no duplication, and concurrency.

So we are going to solve all problems related to security by using one or the other Cryptography technique.

1. Symmetric cipher/Symmetric –key cryptography
2. Asymmetric cipher/Public –key cryptography

* **Assistant Professor in VJES Gholumajra**

This study aims at investigating different Cryptographic techniques and their relevance to today's technology.

KEYWORD: - Symmetric cipher, Asymmetric cipher, security, RSA, Diffie-Hellman Exchange,3-DES,Blowfish,AES

INTRODUCTION

Cryptography is very important and essential technique used in information technology. In the field of cryptography the encryption and decryption is very useful for securing the network (VPN). Different application followed number of method for make data more secure and reliable in different field such as e –commerce, e-banking, e- mail, large scale database. In the next term we start undergo with the basic types of cryptography techniques and algorithms.

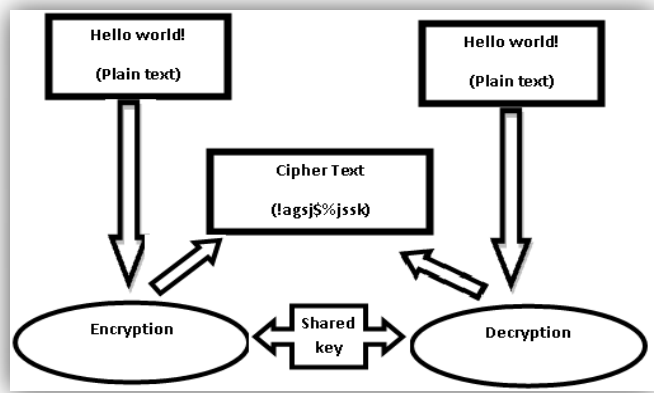


Fig- Encryption and Decryption process

The cryptography is defined in the terms of Symmetric cipher (Symmetric –key cryptography) and Asymmetric cipher/Public –key cryptography. Before start the discussion on above two terms, the original unencrypted data will be referred to as *plaintext* and the encrypted form as *cipher text*.

For example if we have some plain text "ABCDEFGHIJKLMNOP" and we want to convert this data into secure form then by using table method we could rewrite the data into other form called as cipher text.

	1	2	3	4
1	A	B	C	D

2	E	F	G	H
3	I	J	K	L
4	M	N	O	P

Table- Procedure for Encrypt the data

Now after applying encryption the cipher text is comes as resultant "1121314121222324313233441424344"

SYMMETRIC CIPHER

Symmetric cipher is the method in which we can encrypt our data and confidential information very easily, because in this method user and sender could share common key for conversion of plain text into cipher text and vice versa. The strength of Symmetric cryptography is ascertained by the different keys.

Symmetric cipher is further divided into two categories one is steam cipher and second is block cipher

Stream cipher is a method by which we could encrypt one bit or byte of data at a time. Stream cipher is not widely used techniques because its key is to longer than the data. In this plain text acts as input stream and cipher text acts as output stream. At the time of conversion exclusive – OR gate is applied at the input end for secure encryption.

Stream cipher is also known as One-Time Pad which is engaged with purely random key for generating a confidentiality data, but there is one problem in this method the key used for encryption is having large size as comparing with their plain text. For example if an employee wants to transfer 500MB data over a network for encryption the key would be required 4GB long. The problem of stream cipher is overcome by the next method is block cipher.

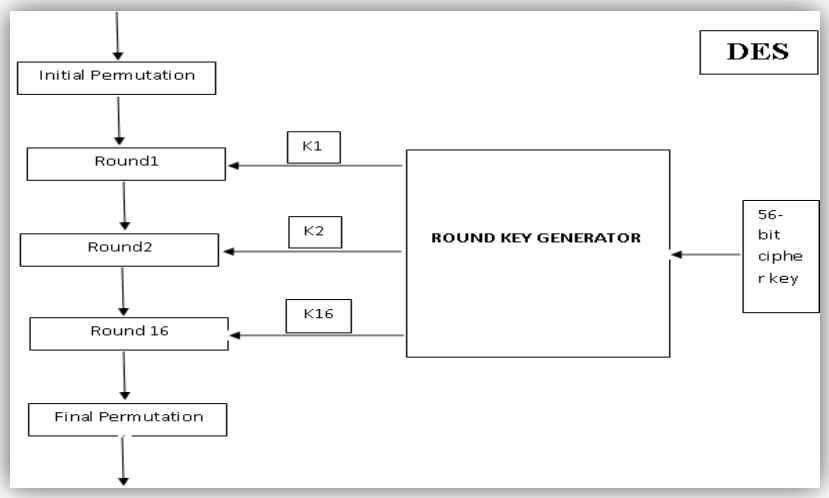
Block cipher is an encryption algorithm which encrypts the full block of data rather than one bit at a time. This technique is more reliable and faster than stream cipher and also more widely used in network security. The block could be in different size like 64 bits, 128 bits, 256 bits and 512 bits etc. The key varies according to the size of block if block size is having 128 bits of plain

text as input with 128 bits of encryption key produce 128 bits of cipher text. In today time generally symmetric block cipher techniques are used for conceal the data. DES, Triple DES, AES, Blowfish, Twofish are most commonly used modus operandi comes under block cipher encryption.

Popular Block cipher:

DES-It is abbreviated as Data Encryption Standard is introduced by National Institute of Standard and Technology (NIST) in US in 1977.DES is an enhancement of Feistel cipher technique. In DES 64-bit is encrypted by 56- bit key because 8 bits are acts as parity bit. The 16 rounds are used in this standard for encrypt the data. The structure of DES is given below:

64 –bit Plain text



64-bit cipher text

Fig- Process of Data Encryption Standard Algorithm

3DES-It is an implementation of DES technique. This method is faster than DES, because this run on 3 time platform. Means if we having 64 bit data then in DES 56 bit key are used but in 3DES the key size is vary three times more and become 168 bit. Sometime the computation becomes very complicated in 3DES. The problem of this cipher is resolved in next method.

AES-AES is abbreviated as Advanced Encryption Standard is mostly used cipher in the world. In this the size of block is 128 bit and its extendable up to the sizes are 192,256 bit. This algorithm is standardized by U.S. Government. It is used on large scale for securing the data

from number of attacks by accepting the brute force and use all possible combination of keys for decipher the data. The security experts believe that AES will be made the standard for securing the data in private era.

Blowfish-Blowfish is imperatively used in all sectors. It is also designed for replace the DES. In this algorithm the plain text is divided into different module and each module is having size of 64 bits, encryption is individually applied on those modules.

Blowfish is very faster algorithm and reliable in producing a better result. Furthermore it is license free that means it is easily available on public domain. Its key range can vary from 32-448 bits. It is monarch's free and unpatented algorithm and it can be found in software for securing the information from third party user with the help of passwords.

The extension of Blowfish is popular as Twofish algorithm .In Twofish 256 bit key is used for ciphering the data. This technique is used in every field either network or database. The example of Twofish such as True crypt, Photo encrypt and GPG.

Camellia-Camellia algorithm is approximately similar to DES algorithms. The main difference between those two methods is cipher round different with each other. Camellia is introduced by Nippon Telegraph and Telephone (NTT) Corporation with Mitsubishi Electric Corporation (MEC) in year of 2000.The encryption key is used in this algorithm having 128,192 and 256-bit. It's implemented on 32-bit processor devices and it can use for small 8-bit application for example smart cards, embedded system. In this algorithm for 128-bit key we used 18 rounds and for 256-bit key used 24 rounds.

In the transferring data over the network SFTP, FTPS, HTTPS and Web DAVS protocols are encrypt via symmetric key ciphers.

ASYMMETRIC CIPHER

Asymmetric encryption is another form of cryptography. This method could be used for authentication and privacy for all application in information security. According to the working

of this algorithm two keys are used for both sender and receiver one is private key and second is public key. When sender sends any information to receiver he/she wants to secure this information so two encryption keys are used at the time of sending and receiving. The public key is used at the sender end for converting the plain text into cipher text. The private key is used by the receiver for reconvert the cipher text into plain text. Both keys are mathematically interconnected with each other and perform their operation. This encryption is very popular with Private Key encryption technique. We are going to start discussion on different category are lies in this algorithm.

RSA- This algorithm is famous from their name because it was developed by three MIT mathematicians **Ronald Rivest**, **Adi Shamir** and **Leonard Adleman**. The basic use of this algorithm is in digital signature and key exchange method. The variable size encryption block and variable cipher key is used in RSA method. Our data is more secure in this method because only those is decode the message who has sufficient knowledge about usage of public key with prime number factor. In this algorithm we use the key pair which is derived from very large prime number, defined by 'n' and that number is the product of two prime number , these prime number may be 100 or more than 100 digits. This technique is used for the security of WSN(wireless sensor network) on a large scale. In WSN data confidentiality, integrity and authentication are three prime factors which are secure by RSA.

The RSA algorithms having basic three phases: ***Key Generation, Encryption and Decryption***

Key Generation Phase (Public/Private key)

1. Select two prime number p and q, but those are not equal to each other ($p \neq q$)

2. Compute $n = p^* q$

3. Then compute function of n $\phi(n) = (p-1)^*(q-1)$

4. Select integer s, such as $GCD(\phi(n),s)=1$ $(1<s< \phi(n))$

5. Compute large integer $d= s\text{-}1(\text{mod } \phi(n))$

6. Public key PBK=(s , n)

7. Private key PVK=(d, n)

Encryption phase

The Public key is used in this phase for converting plain text into cipher text.

1. Select Plain text(T_P)
2. Compute Cipher Text(C_P)

$$\mathbf{C_P = (T_P)^s \bmod n}$$

Decryption phase

The private key is used in this phase for converting cipher text into plain text.

1. Select Cipher text (C_P)
2. Compute Plain text (T_P)

$$\mathbf{T_P = (C_P)^d \bmod n}$$

Diffie-Hellman Key Exchange- The Diffie –Hellman algorithm was introduced by two famous cryptographers named as Whitfield Diffie and Martin Hellman in 1976. The very big advantage of this algorithm was easily transferring of keys at both receiver and send end without any interruption by unwanted user. Because of this feature this algorithms also known as exponential key exchange method.

The Diffie-Hellman algorithm

1. Select two public variable declared as globally one should be a prime number(p) and another one is integer (s) which is subset of (p).

2. Now obtain sender key generation by sender selecting a random integer $X_A < p$ (private) and compute $Y_A = s * X_A \bmod p$ (public).

3. Now obtain Receiver key generation by receiver selecting a random integer $X_B < p$ (private) and compute $Y_B = s * X_B \bmod p$ (public).

4. Encryption at sender end by computing secret key $S_K = Y_B * X_A \bmod p$.

5. Decryption at receiver end by computing secret key $R_K = Y_A * X_B \bmod p$.

Elliptic Curve Cryptography- The first idea about this algorithm was given by Neal Koblitz and Victor S. Miller in year of 1985. The ECC was developed by Certicom and license by Hifn . This working of this technique is based on elliptic curve for produce small, consistent and proficient cryptographic keys. In this algorithm ECC generator is used for generates key with the

help of properties of elliptic curve equation. This method is not widely used as comparing to RSA and D-H because the size of encryption key. ECC is used in many product for the security purpose like 3Com , Motorola, Siemens etc.

The algorithm of ECC has three phases-

Key Generation Phase (Public/Private key)

1. Select a number‘d’ in the range of ‘n’.

2. Compute q= d*p where d= (1 to n-1) and p in the point of curve.

3. Where ‘q’ is act as public key and‘d’ is act as private key.

Encryption

1. Select ‘k’ range from (1 to n-1).

2. Compute two cipher c1=k*p and c2= m + k*q(where m is point of curve)

3. C1 and c2 are cipher text.

Decryption

1. M=c2-d*c1.

2. M is plain text send by sender.

SECURITY

The Security is not a new issue in the Information technology world. It started from the invention of first generation of computers. That means when the computer came in industry, the fundamental of security was also considered with it. The security is defined in different field which are given below

1. Computer security
2. Network security
3. Internet security
4. Information security
5. Data base security

With the invention of computer and mainframe system, theprogrammers have started working on more and more new security technologies.

COMPUTER SECURITY

The computer security is also defined as CYBER security or I.T.security.In the security we have two main basic points

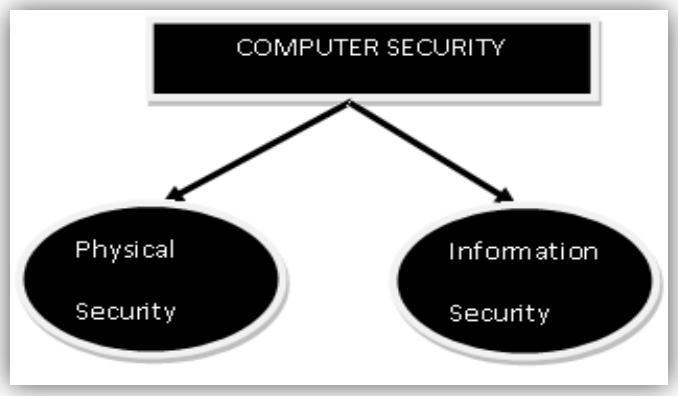


Fig –Types of Computer Security

The first one is physical security which described the prevention methodsfor all equipments and devices on which the programmer and user are working and the other one is information security which is used for data protection.

Physical security is act as a guard for hardware, programs, and network s from physical assets and events that could cause critical damagefor an enterprise, companies, offices or institutions.

The very big example of physical security is CCTV (Closed-circuit television) surveillance, and other basic technology of physical protections also used like security guards, protective barriers, and access control protocols etc.

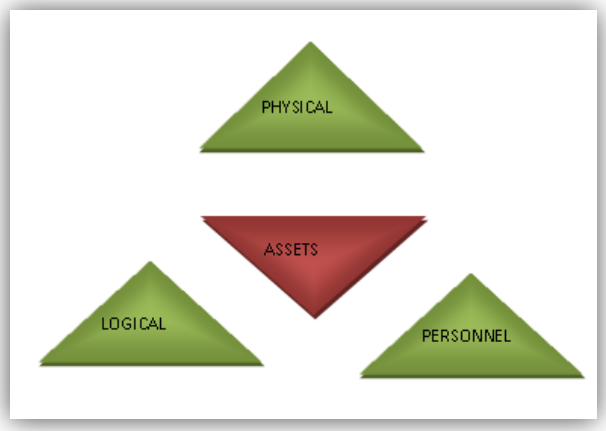


Fig- Assets of Physical security

Now we are going to start discussion about Information security. The information security is defined as info sec for protection of data. It is also known as data security.

The data is collection of real world entities (name, place, etc.).When the raw data is processed it converted into meaningful information. In the computer system data is in the form of table, record, file, structure, so for the protection of this data we use different security methods. For example if we make a data base of our organization by using word processing software and we want to secure our data from the unauthorized user, by using constraints we can easily secure our document.

There are following basic concept of data which are correlate with each other

- Data Integrity
- Data Availability
- Data Authentication
- Data Reliability
- Non – Duplications

For Security of data we use two primitives: Encryption and Decryption

NETWORK SECURITY

Before starting introductionabout security issue of Network it is important to understand we should start with the introduction of network it will help in understanding the concept easily.

The network is the collection of two or more than two computers which are interconnected with each other for sharing any kind of information. Basically we have three types of network

1. Local Area Network
2. Metropolitan Area Network
3. Wide Area Network

The data transfer between one system (node) to another system with the help of communication media which is wired and wireless also.

The very big example of network is Internet, which is widely interconnected.

A LAN is defined as local area network, which having connection between nodes with in local area. it is the network of computers interrelated to each other, sharing the desired information within the organization. In other words, if we want to establish a network in any organization we

preferred local area network.A MAN is defined as Metropolitan area network, which having connection between nodes with in metro cities. Big organizations like baking and insurance companies use MAN to connect and share their information among different locations .A WAN is defined as wide area network. It is very important and useful network, by using this network we share our data from one country to another country very easily. This network is used whole over the world. A WAN is the combination of Local area network and Metropolitan area network. The communication media of WAN network is wireless (SATELLITES).

WORLD WIDE WEB in simple language internet is an example of WAN. It is with the help of internet the total world has been shrink to global table.

For the security of any type of network we used very big technology is called as firewall and IDS (Instruction detection system).

INTERNET SECURITY:

Internet security is of utmost importance as it is spread throughout the world and it is very easy for a computer literate to steal any required information from any web site.Internet security is the branch of computer security. The internet is communication medium by which we can access any information from any area from all over the world. When we transfer our data (packet) from one station to another station we used security token with the head of packet.

There are different types of internet security as given below

1. Network layer security
2. Internet Protocol Security (IPSec)

TCP/IP which stands for Transmission Control Protocol (TCP) and Internet Protocol (IP) aka Internet protocol suite can be made secure with the help of cryptographic methods and protocols. These protocols include Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for web traffic, Pretty Good Privacy (PGP) for email, and IPSec for the network layer security.

CONCLUSION AND FUTURE WORK

The security for any kind of data had become very important. The data privacy is essential query over cloud network. By using number of cryptographic technique we could secure different type

of data in the different aspect. The paper included number of encryption and security method for secure the network, data base, internet and computer system. All above method are very reliable and consistent for the future purpose. This paper is briefly discussed the concept of cryptography techniques and their usage as well as computer security with its categories in sufficient way.

REFERENCES

1. (https://en.wikipedia.org/wiki/Internet_security/ Dated 31dec, 2016, 2:48pm)

2. http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/ Dated-31 Jan 2017 at 3:54pm

3. W .Stallings, "Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA.

4 Reviews and Analysis of Cryptography Techniques Nitin Jirwan , Ajay Singh, Dr. Sandip Vijay Volume 4, Issue3, March-2013

5. https://community.jisc.ac.uk/library/advisory-services/introduction-cryptographic-techniques Dated-31 Jan 2017 at 4:01pm

6. http://www.jscape.com/blog/stream-cipher-vs-block-cipher Dated -1 Feb. 2017 at 10:33 am

7.H. Rodriguez, et al, " Cryptographic Algorithms on Reconfigurable Hardware ", First Edition-1.Springer, (2006), USA.

8. https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm Dated 1 Feb 2017 at 12:07pm

9. W .Stallings, "Network Security Essentials application and standards", Fifth Edition. Pearson Prentice Hall, USA

10. Diffie, W.; Hellman, M. (1976). "New directions in cryptography" IEEE Transactions on Information Theory 22 (6): 644-654.

11. G .Dieter: "Computer Security ", Second Edition. John Wiley & Sons, (2005), UK.

12. Bellare, Mihir; Rogaway, Phillip (21 September 2005). "*Introduction" Introduction to Modern Cryptography*. p. 10.